Information Technology Strategic Plan 2009-2013

DEPARTMENT OF HOMELAND SECURITY
Office of the Chief Information Officer

January 2009

FINAL

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Strategic Plan 2009-2013	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Homeland Security,Office of the Chief Information Officer,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

1.0 Introduction

1.1 Background

The FY2009-2013 Information Technology (IT) Strategic Plan outlines how the Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) will support DHS' mission objectives and goals. It reflects DHS' commitment to focus IT resources on moving forward high-priority operational capabilities, programs, and business processes. The plan articulates DHS IT priorities for developing and delivering capabilities and services to support the mission and business needs of the Department.

The IT Strategic Plan for FY2009-2013 was developed collectively by the DHS Chief Information Officer (CIO) and Component CIOs. The plan emphasizes the use of communication, information, and technology resources to strengthen the pursuit of core DHS goals of protecting America, strengthening preparedness and emergency response, and building unified DHS-wide operations and management capabilities. This plan aligns with the Department's Strategic Plan for Fiscal Years (FY) 2009 – 2013 and, as such, the goals outlined in this plan are directly aligned with those listed in the Strategic Plan. This alignment is illustrated in Table 1 below.

DHS Strategic Goals	**DHS IT Strategic Goals**			
	Goal 1: Establish Secure IT Infrastructure Capabilities to Protect the Homeland and Enhance our Nation's Preparedness, Mitigation and Recovery Capabilities	Goal 2: Strengthen and unify the Department's ability to share information with federal, state, local and tribal partners.	Goal 3: Improve transparency and accountability through effective governance of cross-departmental IT portfolios.	Goal 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT delivery across the Department
Goal 1: Protect Our Nation from Dangerous People	√	√	√	
Goal 2: Protect Our Nation from Dangerous Goods	√	√		
Goal 3: Protect Critical Infrastructure	√	√		
Goal 4: Strengthen Our Nation's Preparedness and Emergency Response Capabilities	√	√		
Goal 5: Strengthen and Unify DHS Operations and Management		√	√	√

Table 1: Strategic Goals Alignment Matrix

IT solutions for the DHS mission are complex. There is a need for increased information sharing, both within and external to DHS, that must be balanced against significant constraints, such as the need for Cybersecurity and lawful protection of privacy and civil rights. DHS must be agile and action-oriented, while simultaneously pursuing the disciplines of IT budgeting, IT governance, enterprise architecture, risk management, and following sound acquisition practices. The IT Strategic Plan prioritizes the path for addressing this complexity while balancing constraints and focusing resources on DHS mission priorities and goals. The Components' IT Strategic Plans, in turn, should align to this Department-wide IT strategic Plan.

Strengths, Opportunities, Weaknesses, and Challenges

Strengths and Opportunities

Within DHS, the Department CIO and the Component CIOs can build on existing IT strengths, which include: a fully functioning CIO Council, a mission-focused IT workforce, an Enterprise Architecture (EA) program with active Component participation, improved collaboration among CXOs, the Department's headquarter and cross-component executive leadership, and strong internal and external partnerships. Though DHS has a relatively small IT talent pool, its composition of Federal staff and contractors comes with strong skill sets. Components have started to leverage Direct Hire Authority, and the Department is working to make this an enterprise-wide practice. With Cybersecurity as a high-priority for the incoming Administration, the DHS IT Community can share its successes in the progress DHS has made in Cybersecurity efforts during its relatively short existence.

There are many internal and external factors that affect the Department at any given time. Both within and beyond the DHS IT realm, the IT community should leverage and take into consideration the following opportunities. Some of these opportunities include the improvement in the number of Federal IT leaders, improving defined information sharing standards, integration among IT and the Acquisition community, enhanced enterprise-level services, and cooperation across the Components for an integrated IT budget approach.

Weaknesses and Challenges

DHS is currently faced with weaknesses that exist both within and outside of its IT space. Weaknesses affecting DHS include a shortage in Federal staff and lack of visibility into enterprise staffing needs. These weaknesses impact IT staffing at the Department and Component levels. A large contributor to the shortage of IT staff is the unnecessarily lengthy clearance processing, which leads to delays in the time that new hires receive their EOD and, subsequently, can start working. Additional weaknesses include the absence of a sound communications strategy internally as well as with external stakeholders. This leads to cumbersome reactionary drills, such as the constant need to respond to Government Accountability Office (GAO), Office of Management and Budget (OMB), and Inspector General (IG) reports. Additional DHS-wide weaknesses affecting the IT community include lack of focus on customer relationship management, inconsistent levels of organizational maturity across the Enterprise, and the absence of Enterprise funding models for shared services. Also, though progress has been made within the DHS IT community regarding Cybersecurity, Identity Management, and the Continuity of Operations Plan (COOP) and Disaster Recovery (DR), new threats are constantly emerging, requiring DHS to continually improve its efforts in these areas.

Specific challenges faced by the IT organization within DHS and across the Components include a relatively immature IT Governance and information sharing governance framework; policy gaps in data ownership and data sharing; shortfalls in security access regulations for shared services; and difficulties associated with

recruiting and retaining qualified IT professionals. Additionally, many within the current contract support personnel are inexperienced in handling the many different types of contracts on programs across the Enterprise.

Other challenges faced by DHS simply stem from the fact that the organization is still relatively new and young. Despite this, DHS recognizes that, although continued improvements have been made, it still needs to strengthen its capabilities. Areas of focus include further optimization of IT infrastructure, strengthened Cybersecurity and secure information sharing, improved management of capabilities and prioritization of critical activities, alignment of priorities to available funding, clearly defining COOP and DR requirements. Additional challenges include retaining highly qualified IT professionals and leveraging of Enterprise IT Services. Doing so would likely increase the flexibility of the Department and improve mission performance, among other benefits.

State of the DHS IT Infrastructure

DHS made a commitment in 2003 to integrate, consolidate, and transform the individual Component infrastructures into an integrated, world-class IT infrastructure capable of supporting the significant demands of the Enterprise. To date, DHS has made great strides in achieving this integrated IT structure. The initiatives in place or scheduled for production in FY 2009 to achieve this include: creation of one secure network, reduction of the number and transformation of data centers, establishment of common and reliable e-mail communication, establishment of a unified IT acquisition process, implementation of Single Sign-On network access, compliance with Federal Desktop Core Configuration (FDCC) standards, and consolidation and strengthening of communications security.

1.2 DHS IT Vision

DHS is a world-class leader in technology that provides secure, pertinent, and timely information to the right people to promote a secure America.

1.3 DHS IT Mission

To provide DHS and its partners the IT services required to lead the unified national effort to prevent and deter terrorist attacks; and protect against and respond to threats and hazards to the Homeland.

1.4 Authority

The DHS IT Strategic Plan has been developed under the authority of the DHS CIO. The DHS OCIO derives its authority from the Clinger-Cohen Act and Management Directive (MD) 0007.1. This Management Directive establishes the DHS vision, as well as the authorities and responsibilities of the Department's CIO. At the Federal level, U.S. Code Title 44, Public Printing and Documents, Federal Information Policy mandates that the CIO develop and maintain a strategic information resources management plan; establish goals for improving the contribution of information resources to program productivity, efficiency, and effectiveness; and identify methods for measuring progress towards reaching those goals.

The DHS OCIO is the organization that manages and directs the Department’s IT functional area. This office is headed by the DHS CIO who is directly supported by the CIO staff functions and the CIO Council. The Department's CIO is the line of business (LOB) chief who exercises leadership and authority over IT policy and programs DHS-wide. The DHS OCIO has aligned its goals to Federal and Department-wide guidance in order to enhance mission execution. The guidance listed in table 3 in the Appendix shaped the goals, objectives, and key initiatives defined in this plan.

The President and Congress directed DHS to perform an essential and multi-faceted mission: prevent and protect against terrorist attacks; respond to man-made and natural disasters; perform the law enforcement and other crucial functions of the Department's component agencies; and play a central role in augmenting the Nation's ability to gather, analyze, and disseminate information and intelligence. As such, DHS and Component CIOs are charged with helping to facilitate the multi-faceted mission by delivering world-class IT services. The table in Appendix A provides additional Authorities, as well as Federal and Departmental Guidance.

2.0 Roles and Responsibilities of the DHS and Component CIOs

The OCIO is a critical transformation entity in the Federal government. The CIO position was established by the Clinger-Cohen Act of 1996 as the key factor in closely aligning agency IT investments with agency mission goals and objectives. Congress established this position with the intention that the CIO would be an executive leader serving as a member of the agency's top-level management team, assisting leadership in translating business needs into IT investments. The Clinger-Cohen Act of 1996 charges Federal Government CIOs with responsibility for supervising and coordinating the design, acquisition, maintenance, use, and disposal of IT by agencies and for monitoring IT program and activity performance.

This mandate was further codified in OMB's Circular A-130, which outlines in detail the processes that an agency must implement to fulfill Clinger-Cohen Act requirements. To address the issues specific to IT investments within DHS, the DHS OCIO established MD 0007.1, which states that the OCIO has the authority to guide IT investment spending throughout DHS. To accomplish this, the DHS CIO has implemented a requirement that IT spending by Components must be approved by either the Component-level CIO or the DHS CIO, depending on the dollar threshold in the MD. The directive also institutes an unofficial, "dotted-line", reporting for Component CIOs to the OCIO at DHS headquarters, in addition to their formal direct reporting to Component heads. MD 0007.1 supports and expands on Clinger-Cohen Act requirements requiring executive agencies to develop a Capital Planning and Investment Control (CPIC) process for making technology, budget, financial, and program management decisions.

The importance of the DHS mission and the current focus on effective information sharing and management makes the DHS CIO and Component CIOs even more critical. Since the September 11, 2001 attacks on the Homeland, Congress and various Executive Orders from the President mandating improved and enhanced information sharing between Federal agencies, and with state, local, tribal, and private industry partners, as well as foreign governments have made the CIOs' role essential to achieving the mission.

Component CIOs, like the DHS CIO, are responsible for overseeing their organizations' IT investments. The Component CIOs focus on meeting their respective mission IT requirements and providing high quality service to their business customers. Additionally, they are responsible for instituting IT investment management and governance practices that align with those of the Department.

Within DHS, there is a federated, yet collaborative structure to ensure that there is standardization, consolidation, and sharing of both infrastructure and solutions across the Department in cases such as IT infrastructure, enterprise services, administrative support systems, data and information sharing, and records management.

3.0 Key Drivers for an Integrated DHS IT Strategic Plan

3.1 Mission-Driven Information Technology

The United States continues to face increasing domestic and foreign threats. Consequently, DHS must be agile and technologically proficient to successfully prevent, respond to, recover from, and mitigate these threats. To meet these challenges, the DHS Strategic Plan identifies overarching strategic goals around protection, emergency response, and management improvements.

IT is essential to the Department's success in meeting these strategic goals. A secure and properly structured IT organization is one of the greatest force multipliers available to the Department. IT is a crucial organizational asset that must be strategically developed, deployed, and used as an integral part of mission accomplishment. IT aids in facilitating the processes and activities necessary to carry out the mission. IT also provides new and improved capabilities to gather, analyze, and securely share intelligence/ Sensitive Compartmented Information (SCI), Sensitive But Unclassified (SBU), and unclassified information with Federal, state, local, tribal, and foreign partners. IT allows DHS to provide prompt, accessible, and reliable services to customers and to efficiently and effectively carry out internal business practices. IT also provides the communications and computing infrastructure that allows for continuity of operations and rapid response in emergency and surge situations.

3.2 OMB Direction, Congressional Mandates, and Government-wide Initiatives

DHS is committed to supporting and leveraging Federal Government-wide initiatives such as the OMB E-Government (e-Gov) Initiatives and LOBs. Operated and supported by Federal agencies, these initiatives provide high-quality and well-managed solutions for e-training, grants management, etc. These e-Gov services and processes establish a broad framework of measures that require using Internet-based IT to enhance citizen access to government information and services.

DHS supports the government-wide Government Performance and Results Act (GPRA) initiative to provide for the establishment of strategic planning and performance measurement in the Federal Government. This plan is in support of GPRA and the Departmental initiative to improve strategic planning across the Department. Additionally, DHS participates in the President's Management Agenda (PMA) Initiatives and the Program Assessment Rating Tool (PART) program whose aim is to improve program performance across the Federal government. Specific to IT investments, DHS also adheres to requirements in the OMB Circular A-130 and those of the Exhibit 300 reporting process.

In 2006, OMB initiated the development of the IT Infrastructure LOB Initiative. Targeting the approximately $24 billion in IT infrastructure, operations, and management spent across the government, the idea is to drive consolidation, standardization, and optimization through establishing benchmarks for cost and service levels by holding agencies accountable for performance improvement against these benchmarks. Because this initiative, like other E-Gov initiatives, is not fully funded, it is up to DHS to work towards establishing and implementing an IT environment of shared IT services. This consolidated infrastructure and shared services is the vision for the Infrastructure Transformation Program at DHS and is the means by which to reduce IT commodity expenditures and free up funding for direct mission support. Goal 1 in Section 4.0 of this document highlights the Department's commitment to optimizing the IT infrastructure.

DHS has made significant progress in standing up EA and delivering enterprise solutions. The DHS EA Program Management Office (PMO) is currently in the process of rolling out guidance from OMB on the use of Segment Architectures. As a relatively new agency, DHS operates under even more scrutiny by the GAO,

OMB, and Congress than the other agencies do. Additionally, legacy programs are under the watchful eye of the IG. It is incumbent upon DHS to increase visibility into and improve performance of its IT programs since the Department's IT budget comprises a fairly significant portion of the DHS budget. In FY09, the DHS IT Budget is estimated to be about 13% of the overall DHS Budget.

GAO, OMB, and Congress have watched DHS closely since the agency's inception to help ensure that the appropriate level of oversight over billions invested in its programs. Annually, GAO conducts an investigation and provides a report to Congress regarding the oversight of major programs within DHS. Though there is still plenty of progress to be made at DHS, positive steps have been taken to ensure programs are managed appropriately. Across the Department, several initiatives have been put in place by the Under Secretary for Management to improve performance of programs including the reengineering of the Department's Acquisition Directive (D-102-01), establishment of an Acquisition Review Board to conduct acquisition reviews, and development of a strategic requirements planning process. Additionally, the OCIO has instituted IT acquisition reviews and EA Review Board (ERB) reviews of DHS IT programs, and is currently in the process of establishing an integrated IT Governance framework.

3.3 Federated Organizational Structure

DHS was established to bring autonomous Components together with oversight from one Headquarters organization. This federated organizational structure poses challenges with the benefits it brings. For example, the DHS CIO and Component CIOs must work closely together to ensure alignment of governance processes and investment management practices. Additionally, the oversight authorities over programs are shared by both DHS and Component Leadership. At DHS, efforts are underway to institutionalize an IT portfolio approach. This, in addition to establishing Segment Architectures, in accordance with the OMB guidance provides increased visibility into all IT spending. This would help the Department to eliminate gaps, reduce redundancies, and optimize resources through reuse and promotion of enterprise services.

3.4 Trends in the Federal IT Community

Technology advances are increasing performance and capability. Those advances must be properly engineered and deployed to balance access and security since DHS customers demand near instant access to complex data sets that are fully integrated and presented to mission operators. These data sets must be in a readily accessible and understandable format that can be translated into immediate action. A trend in technology that hinders the Department's capabilities is the increasing scarcity of the most highly skilled technology employees. The IT community is lacking IT professionals that possess the business transformation, architecture, security and privacy, and management skills, in concert with the right level of experience, to leverage technology trends and understand and meet customer demands for technology support in the mission context.

DHS is committed to working strategically to ensure that IT is optimized and that technology trends are leveraged in a way that allows DHS to focus on its mission support roles, as opposed to duplicating commodity technology services and products.

3.5 Budgetary Constraints

DHS continues to face major challenges in funding the technology needs for its mission-specific requirements while at the same time providing IT infrastructure and overall support services. Many requirements within the Department and across the Components argue for increased IT investment. However, this contradicts the overall trend of reduced spending by the Federal government. As the Department matures, governance over IT spending is improving. Planning and budgeting for IT investments

must continue to improve so that all mission and business needs can be successfully met and appropriately planned.

"Above – guidance" requests have been the vehicle for programs to include budgetary requests above what was originally intended for the program, or its "within guidance" request. Increased focus around IT infrastructure consolidation has resulted in increased "above guidance" requests. Much of the DHS FY10 IT budget increases are the result of "above guidance" requests that were approved the Deputy Secretary during the budget review in Spring of '08. The DHS Infrastructure investment requested additional funding in FY10 predominantly for Data Center migration, Cybersecurity, and Network consolidation efforts. The common themes seen in the funding requests are tactical communications, information sharing and interoperability efforts, as well as infrastructure consolidation efforts. The overall requested DHS IT budget increase from FY09 to FY10 is roughly $1.6 billion. Figure 1 below illustrates the requested IT budget by mission and business objectives.

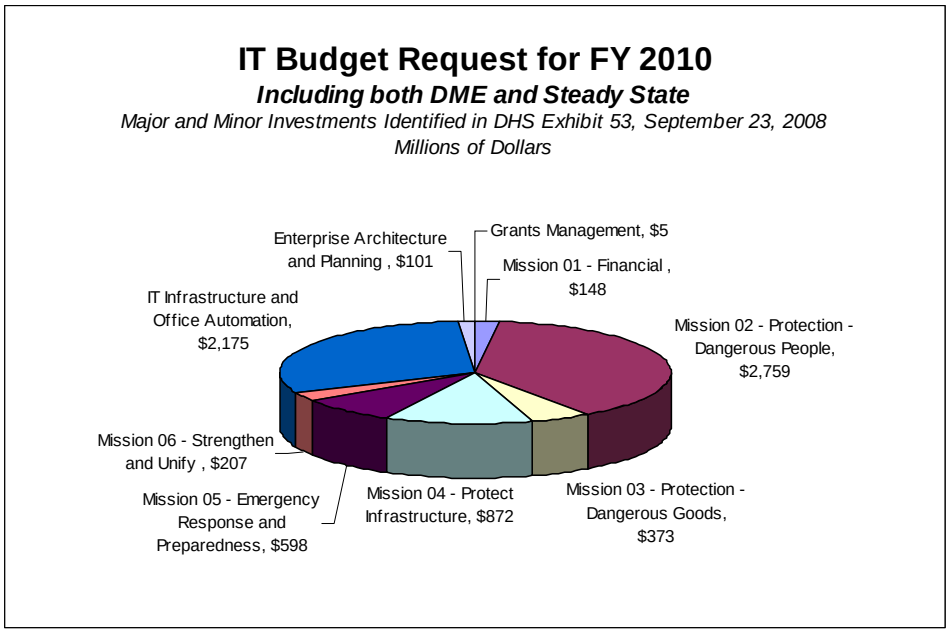

Figure 1: FY2010 IT Budget Request for Development/Modernization/Enhancement and Steady State Programs

The Department is focused on improving transparency in IT spending, as well as increased effectiveness and efficiency of its IT programs. As such, the DHS CIO has made a secure IT infrastructure a top priority. The DHS CIO and Component CIOs are working together to improve the IT portion of the Integrated Planning Guidance (IPG) to better inform the IT Planning, Programming, Budgeting, and Execution (PPBE) process.

4.0 Strategic Goals, Objectives, Metrics, IT Priorities, and Enterprise Initiatives

A maturing DHS as well as improved integration across Component organizations have allowed for this Departmental IT Strategic Plan and improved efforts across the IT community around planning, programming, budgeting, and execution. The Key Drivers in the previous section provide additional support for the need to move the Department's IT community towards a more strategic direction. The strategic goals

and objectives included in this section are envisioned to aid in achieving a more efficient IT management and governance approach and better coordination among Departmental stakeholders.

This section of the IT Strategic Plan identifies the CIO community's strategic goals, objectives, and the priorities and initiatives intended to achieve them. The focus of this section is around the Enterprise IT services for which the DHS CIO and Component CIOs are responsible. The objectives listed support the achievement of the goals, and the corresponding metrics are intended to gauge whether the objectives were met. For each of these objectives, IT priorities and near, mid, and long term initiatives are provided. These are the actions to be carried out to provide the Enterprise with needed IT services and ultimately achieve the Department's objectives and IT strategic goals. The table below summarizes the alignment of the IT strategic goals and objectives discussed throughout this section.

Table 2: Strategic Goals and Objectives

Goals	Objectives
GOAL 1: Establish secure IT infrastructure capabilities to protect the Homeland and enhance our Nation's preparedness, mitigation and recovery capabilities.	Objective 1.1: Optimized IT Infrastructure
	Objective 1.2: Strengthened Cybersecurity
GOAL 2: Strengthen and unify the Department's ability to share information with federal, state, local and tribal partners	Objective 2.1: Secure and Trusted Information Sharing
	Objective 2.2: Enhanced DHS Person Screening and Credentialing Capabilities
GOAL 3: Effectively manage IT capabilities and implement cross-departmental IT portfolios that enhance mission and business performance.	Objective 3.1: Integrated Departmental Governance
	Objective 3.2: Enhanced Departmental IT Strategic Sourcing and Vendor Management Capabilities
	Objective 3.3: Enhanced Communications
GOAL 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT delivery across the Department.	Objective 4.1: Comprehensive and Effective IT Human Capital Management

GOAL 1: *Establish secure IT infrastructure capabilities to protect the Homeland and enhance our Nation's preparedness, mitigation, and recovery capabilities.*

DHS must enhance, maintain, and optimize IT services and resources to carry out the Department's mission to protect our nation from dangerous people and goods. It is imperative that DHS achieve the following:

- Protect our nation's critical infrastructure and strengthen DHS Cybersecurity capabilities

- Establish a secure, unified and comprehensive network architecture for sharing classified intelligence and homeland-security information throughout DHS, consistent with both DHS and DNI architecture frameworks
- Provide IT solutions and support for those who protect America
- Develop and integrate a unified IT infrastructure for supporting the department's mission requirements
- Implement capabilities for preparedness and emergency response. Strengthen IT agility and resiliency to support emergencies, disaster recovery, and nonstop performance of IT and communications, and
- Improve communication and IT capabilities for DHS personnel working in remote locations.

The DHS CIO Council, which consists of the CIOs from all DHS Components and major Headquarters organizations, prioritized IT infrastructure domains to achieve strategic goals, improve customer satisfaction, and reduce overall IT infrastructure cost. The areas of the DHS IT Infrastructure identified for priority implementation include network services, data centers, E-mail services, desktop services, and implementing a Single Sign-On capability.

Objective 1.1: Optimized IT Infrastructure

IT capabilities can help to mitigate the risks inherent in natural disaster, terrorist, and criminal threats. As such, the IT infrastructure must be optimized to increase the resilience and quality of the infrastructure so that the Department's ability to reduce risk and deliver services is strengthened. A critical factor of quality infrastructure services delivery is the ability to support expected levels of system restoration and Continuity of Operations in the event of man-made or natural disasters. The Department must continue to move towards common infrastructure services. It can do so by continuing to leverage the HLS EA to characterize the Department-wide infrastructure portfolio and identify opportunities to standardize, consolidate, and ultimately optimize the infrastructure. The Department is in the process of implementing OMB guidance on Segment Architectures in the FEA Practice Guidance (see section 2.1.1 for additional information), which will also contribute to ensuring IT investment alignment, infrastructure consolidation, reduction in duplication of IT capabilities, and achieving economies of scale.

Currently across the Department, many systems have become highly complex, requiring highly trained technical and administrative personnel in different Components and employing various COTS packages that either have the same capabilities or address similar needs. These systems conform to different standards, rarely share information with each another, and are often isolated within the Component. Consolidating infrastructure such as data centers, networks, and e-mail services will improve product quality and

performance, security and COOP compliance, and will result in more competitive pricing, product range and flexibility, improved deployment reliability/delivery speed, and enable adequate post-migration support.

The IT Priorities in support of this objective are as follows:

1.1.1: Achieve Data Center Consolidation - The Department is continuing efforts to move from 17 legacy data centers to two large-scale enterprise data centers. The two data centers are known as Stennis and Electronic Data Systems (EDS).

Metrics for determining successful achievement of this priority include:

- Number of legacy data centers remaining
- Percentage of Trusted Agent FISMA (TAF)-listed systems/major applications housed in one of the two data centers

Enterprise Initiatives for the Near-Term (within one year):

- Continued migration of legacy data centers
- Provide Internet Protocol version 6 (IPv6) capability (DNS, DHCP, NTP, etc) at data centers
- Establish C-LAN data backup in the DHS enterprise data centers.
- Integrate Service Level Agreements (SLA) into Memorandums of Understanding (MOU) with our partners

The Department intends to complete the relocation of legacy data centers to the enterprise data centers by FY2011. Upon completion of the data centers' co-location, the Department will be moving in the direction of virtualization and then establishing common computing services as a unified enterprise strategy. Common computing services offer reduced operational costs, improved scalability, improved utilization of IT assets, faster deployment times, and consolidation of hardware and software maintenance.

Measures for successful establishment of common computing services include the increase in number of DHS business applications utilizing server virtualization and managed services.

Enterprise Initiatives for the Mid-term (2-3 years):

- Co-location of application services at the two data centers

Enterprise Initiatives for the Long-term (4-5 years):

- Establishment of email archiving capability and integration and implementation of virtualization and cloud computing.

1.1.2: Achieve Network Consolidation- The Department is continuing efforts to consolidate all legacy networks to one enterprise-wide, integrated network called DHS OneNet.

Metrics for determining successful implementation of this priority include:

- Number of WANs transitioned to DHS OneNet
- Percentage increase in circuits transitioned to DHS OneNet
- Percentage of sites migrated to MPLS
- Percentage of sites under DHS NOC control
- Percent of hardware/software applications (or general support systems) that are IPv6 capable

Enterprise Initiatives for the Near-Term (within one year):

- Promotion of integrating DHS Wireless systems onto a common OneNet backbone—per DHS guidelines

Enterprise Initiatives for the Mid-term (2-3 years):

- Transition of five WANs to a single network in the mid-term

Enterprise Initiatives for the Long-term (4-5 years):

- Establish a backup DHS OneNet NOC/SOC, establish e-mail archiving capability
- Establish IPv6 infrastructure to align DHS with OMB IPv6 implementation requirements
- Upgrade and modernize DHS wireless systems to meet operational needs, narrowband mandates (e.g., P25), interoperability, and security requirements (e.g., AES encryption)—per DHS MD 140-01 and NTIA narrowband mandate

1.1.3: Establish Disaster Recovery and COOP Capabilities across the Enterprise - The Department is in the process of creating a more efficient IT environment that includes additional disaster relief and recovery capability at the two target data centers.

Metrics for determining successful implementation of this priority include:

- Percentage increase in critical systems with successfully-tested Disaster Recovery and COOP capability based on the approved Business Impact Analysis (BIA)
- Percentage of successfully tested plans according to FISMA requirements in the last 365 days
- Increase in number of structured data elements that support critical information transfer across systems
- Percentage increase in number of systems that are available with maximum recovery time

Enterprise Initiatives for the Long-term (4-5 years):

- Implement of Disaster Recovery and COOP capability
- Complete the co-location of data centers
- Enable DR capabilities for ICE, USCIS, US-VISIT, USCG, and HQ at the Stennis and EDS data centers

1.1.4: Implement common secure communications (voice/video) capability- Establishing a common secure communications capability will allow the Department to meet requirements for routine and crisis communications across DHS and with Federal, State & local partners.

Metrics for determining successful implementation of this priority include:

- Percentage of DHS and state, local, and tribal officials with the requirement for real-time voice/VTC collaboration who can be connected via the common capability

Enterprise Initiatives for the Near-Term (within one year):

- Implement DHS Tactical Interface Gateway (TIG) at Top Secret (TS) level
- Develop enterprise requirement for secure communications capability (including validated requirements for communications with state, local, and tribal partners)

Enterprise Initiatives for the Mid-term (2-3 years):

- Meet basic NCCC requirements for secure voice/VTC connectivity to State Local and Tribal officials
- Implement TIG at Secret level

- Complete COMSEC Modernization

Enterprise Initiatives for the Long-term (4-5 years) include:

- Complete implementation of Secure Communications target architecture

Objective 1.2: Strengthened Cybersecurity

Strengthened Cybersecurity is a top objective for DHS. Cybersecurity is a critical attribute that permeates all the processes of an organization and enables an effective, safe environment for carrying out the mission, sharing information, and conducting business. Identity management and access control have been identified as important elements of Cybersecurity and information sharing and, consequently, is the primary focus of this IT Strategic Plan. DHS is continuously strengthening IT security and is currently leading an effort to implement user authentication and Single Sign-on (SSO) network access.

Adherence to Cybersecurity standards to marginalize Cybersecurity attacks is fundamental to successfully carrying out mission and business requirements at DHS. Therefore, great importance has been placed on the IT community's efforts to meet these standards.

The IT Priorities in support of this objective are as follows:

1.2.1: Achieve FISMA Compliance - The Federal Information Security Management Act (FISMA) requires DHS to develop, maintain, and annually update an inventory of information systems operated by the Department or under its control. It is imperative to ensuring the security of information and systems that DHS systems be in compliance of FISMA requirements.

Metrics for determining successful implementation of this priority include:

- Maintaining a "green" status on the annual FISMA Scorecard (by meeting FISMA requirements)
- Percentage of systems with a valid accreditation

Enterprise Initiatives for the Near-Term (within one year):

- Develop an enterprise security plan

Enterprise Initiatives for the Mid-term (2-3 years):

- Develop Component IT Security Strategies

1.2.2: Enhance Secure Communications and Security Operations Center Capabilities – Enhancing secure communications and SOC capabilities is a top priority for DHS because it is critical to sustain effective, efficient, reliable, and affordable DHS IT systems.

Metrics for determining successful implementation of this priority include:

- Percentage of circuits converted to the Homeland Secure Data Network (HSDN)
- Number of circuits converted to Multiprotocol Label Switching (MPLS)

Enterprise Initiatives for the Near-Term (within one year):

- SAML 2 compliance
- Deploy secure DNS
- Complete Phase I and Phase II of National Security Systems Joint Program Management Office (NSS JPMO)
- Develop the Trust Zone and Policy Enforcement Point (PEP) Implementation plan

Trust Zones are subject to a common security policy and rules governing who and what systems have access to data and services. PEPs provide capabilities such as firewalls, malware detection, and intrusion detection within the Trust Zone architecture.

1.2.3: Establish Internal and External Identity and Access Management (IDAM) - Identity and access management are paramount to ensuring Cybersecurity.

Metrics for determining successful implementation of this priority include:

- Percentage of users using Active Directory
- Percentage of TAF-listed applications using App. Authentication/Single Sign-On
- Percentage of HSPD-12 cards issued
- Percentage of HSDN users and applications using Attribute Based Access Control (ABAC) access-control facility

Enterprise Initiatives for the Near-Term (within one year):

- Enterprise active directory implementation

Enterprise Initiatives for the Mid-term (2-3 years):

- Establish HSPD-12 Logical Access Controls and single sign-on implementation (including federal, state, local and tribal partners)
- Implement strong authentication and ABAC capability in the HSDN Secret environment, aligned and interoperable with major Committee on National Security Systems partners

Enterprise Initiatives for the Long-term (4-5 years):

- Establish access controls at the data-level
- Fully implement IDAM capability across the Enterprise

1.2.4: Implement OMB Cybersecurity Requirements – DHS will continue to implement Cybersecurity initiatives in accordance with OMB requirements, including implementation of a secure desktop platform that supports the Department's mission-based requirements, reduction of external connections through the Trusted Internet Connection (TIC) initiative, and compliance with the FDCC initiative across the Federal government to standardize desktop images. This will provide a means for improving information security and reducing overall IT operating costs.

Metrics for determining successful implementation of this priority include:

- Percentage of Component IT Security strategies developed
- Percentage of points of presence (POP) going through the TIC
- Percentage of traffic going through the TIC
- Percentage of desktops that have been reconfigured in accordance with FDCC.

Enterprise Initiatives for the Near-Term (within one year):

- Consolidation of connections to the TICs
- Beginning FDCC implementation

Enterprise Initiatives for the Mid-term (2-3 years):

- Develop Component IT Security strategies
- Complete the FDCC implementation across all of HQ and the Components

GOAL 2: Strengthen and unify the Department's ability to share information with federal, state, local and tribal partners.

DHS must maintain and strengthen the IT infrastructure that enables information sharing to support DHS and trusted partners. The goal of the DHS Information Sharing Environment (DHS-ISE) is to "get the right information to the right person at the right time" and in a usable format that ensures the information is available and actionable. Figure 2 below depicts the target DHS ISE.

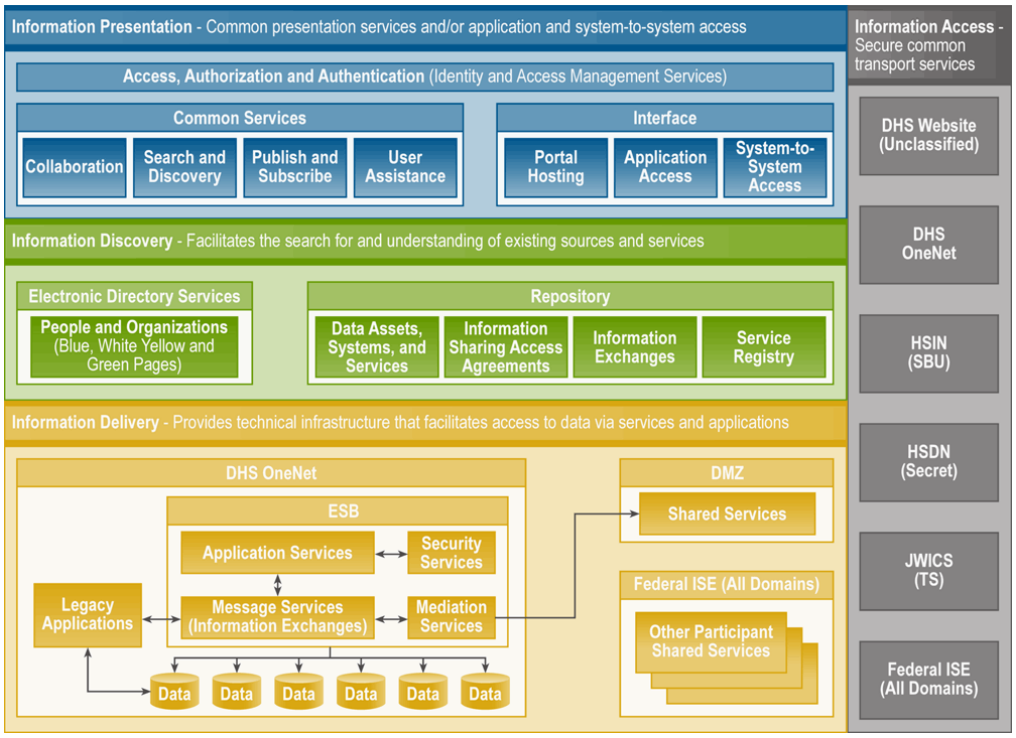

Figure 2: Target Information Sharing Environment

DHS leaders must actively promote the culture, focus, and participation required to achieve the target DHS-ISE, including reinforcing the requirement to share information while protecting the privacy and civil liberties of citizens; ensuring the investments and resources support the plans and guidance to transition to and sustain information sharing goals and targets; building necessary relationships and agreements with partners in the Department as well as the Federal, state, local, tribal governments, and the private sector; and supporting participation in cross-organizational and external communities responsible for promoting and implementing information sharing.

Program and project managers must put information sharing practices in place while ensuring they are consistent with applicable laws, policies, standards, and agreements. IT managers must also understand Federal and Department information sharing goals, measures, guidelines, and requirements; define and manage the risks associated with information sharing; actively participating in communities of interest to contribute to the creation of shared processes, practices, and vocabulary; and understand current information sharing assets and services that can be reused or leveraged.

Objective 2.1: Secure and Trusted Information Sharing

DHS is currently in the process of implementing a comprehensive approach to measuring the effectiveness of Departmental information sharing. The Department has developed and is currently tracking milestones for each of the information sharing priorities and the institutional infrastructure that will enable DHS to create the secure and trusted environment necessary for information sharing.

The DHS Information Sharing vision includes an effective information sharing environment that virtually and securely connects mission partners who span the full spectrum of functional areas needed to secure the homeland. The target DHS-ISE is intended to provide an information sharing interface that lets users appropriately find and access the people and data necessary to perform their job.

The IT Priorities in support of achieving the information sharing objective are as follows:

2.1.1: Develop Segment Architectures for Priority Segments in accordance with the Functional Areas defined by the Office of Policy/Office of Strategic Plans – The Department is required to execute a broad set of missions to meet its homeland security goals. The DHS EA, developed and base-lined by the DHS CIO with input from the DHS Components, organizes the Department's mission space around "Functional Areas", also known as the DHS enterprise segments, and is illustrated in Figure 3 below. The EA team facilitates the further development of the target enterprise by engaging with the DHS Components. The Office of Strategic Plans has adopted the identified functional areas to serve as a neutral lens by which to plan and identify mission-supported strategic requirements and capabilities. These Functional Areas also serve as portfolios to designate groupings of activities, assets, programs, projects, and other resources around groups of similar functions. Each of the Functional Area groupings are designed to encompass the mission spaces of multiple Components, thereby helping to illuminate areas where cross-Component coordination and integration could be beneficial to the Department's missions. They also help provide DHS-wide transparency into what the Department does and the resources it needs to accomplish its missions.

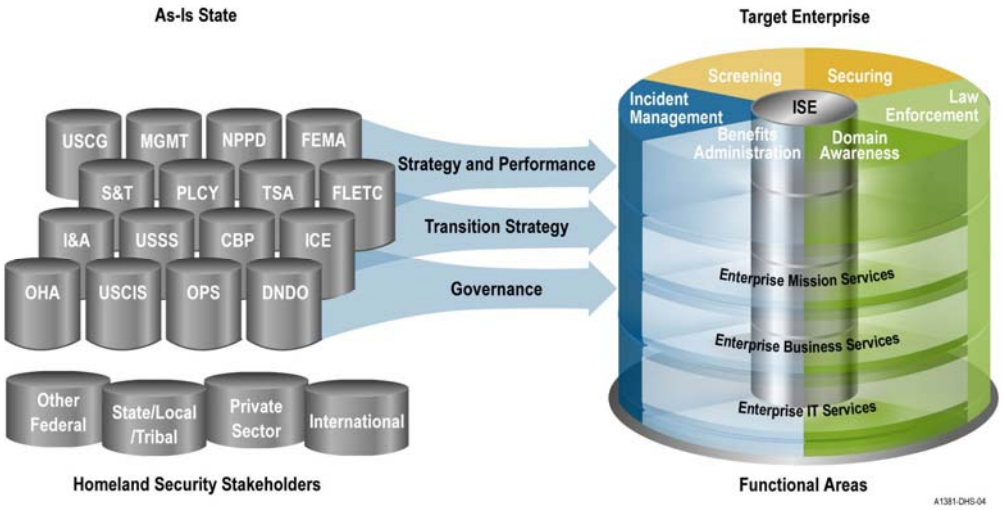

Figure 3: As-is and Target Enterprise for DHS

DHS has identified the following as priority segment architectures for FY09:

- Law Enforcement
- People Screening
- Information Sharing

- Human Capital
- Geospatial
- Networks
- Email

Metrics for determining successful implementation of this priority include:

- Proportion of segments with business driven Integrated Project Teams
- Number of segments that have business and technical target solutions defined through segment architecture analysis
- Number of segments that have transition strategies, with performance goals, for reaching the target solution
- Number of investments within each segment that support the target solution (goal is 100%)

Enterprise Initiatives for the Near-Term (within one year):

- Continue to develop and implement solutions for the existing segments, including building out the Information Sharing Segment Architecture to include information sharing for Identity and Access Management, Infrastructure, Screening, and Law Enforcement
- Develop a Person Centric View (PCV) implementation and transition strategy and related privacy framework for major mission component user and programs

Enterprise Initiatives for the Long-term (4-5 years) include:

- By 2013, DHS plans to develop segment architectures for all portions of the enterprise

As DHS builds out the remaining segments, focus will remain on establishing enterprise cross-domain solutions and implementing the governance mechanisms appropriate to manage cross-segment investments.

2.1.2: Develop a DHS Information Sharing Environment Supporting the DHS Functional Areas and Aligned with PM-ISE Priorities - The target DHS-ISE has been defined to operate within the larger cross-Federal information sharing environment defined by the Office of the Director of National Intelligence's (ODNI) Program Manager for the Information Sharing Environment (PM-ISE). The DHS-ISE will extend the scope of DHS information sharing to encompass the full range of its responsibilities in the functional areas required to achieve its mission.

Metrics for determining successful implementation of this priority include:

- Percentage of initiatives negotiating or updating information sharing access agreements with external partners compliant with the One DHS policy
- Percentage of initiatives developing cross-Federal information exchange standards
- Percentage of initiatives providing artifacts used to search for and understand sharable resources and services
- Percentage of applicable processes and services supporting a common framework for key PM-ISE initiatives, such as Suspicious Activity Reports (SAR); Alerts, Warnings, and Notifications (AWN), and Terrorist Watch List (TWL)

Enterprise Initiatives for the Near-Term (within one year) include:

- Develop architecture, policies, and governance to support the transition to the target DHS-ISE, compliant with PM-ISE guidance, standards, and segment architectures

- Establish Initial Operating Capability for Information Sharing Discovery Services as part of the target DHS-ISE
- Establish DHS Enterprise Service-Oriented Architecture (SOA) Message Header Framework as a component of the DHS-ISE strategy

Enterprise Initiatives for the Mid-term (2-3 years) include:

- Implement Full Operating Capability for Information Sharing Discovery Services
- Implement DHS Enterprise SOA Message Header Framework as a component of the DHS ISE strategy
- Establish a funding strategy and governance framework to implement an enterprise-wide service-oriented architecture that supports reuse of resources, development of standard information exchanges, and complies with Federal information sharing standards

2.1.3: Institutionalize data management, data accessibility, and data protection policies- DHS is leading multiple efforts to facilitate data management maturity within the Components as a means for promoting information sharing with data that is visible, understandable, accessible, trusted, and interoperable. DHS will mature through the development of Data Management Plans, implementation of Data Stewardship and development of Data Performance Measurements.

Metrics for determining successful implementation of this priority include:

- Percentage of systems with data described and available for discovery within DHS ISE Common Framework
- Percentage of Major IT Programs adopting or implementing NIEM for information exchange standardization
- Percentage of Major IT Programs implementing Data Management Plans, Data Stewardship and Data Performance Measurements
- Percentage of relevant DHS systems compliant with the target data architecture for the People Screening Segment to include the Credentialing Framework Implementation and Transition Strategies
- Percentage of Components compliant with supporting data safeguards for protection of privacy or sensitive information in support of the SOA Framework

Enterprise Initiatives for the Near-Term (within one year):

- Improve visibility of Section 508 compliance of Department-wide IT via TAF reporting tool, quarterly web assessments, and Component-level accessible technology programs
- Ensure electronic information and data are fully accessible to members of the public and employees with disabilities, including emergency incident information as this information is often of critical relevance to persons with disabilities
- Improve Department-wide governance related to compliance with Section 508 by strengthening oversight and review via standard IT life-cycle processes
- Improve Department-wide selection and use of IT products to meet Section 508 compliance requirements by conducting hands-on assessments of items before release to employees
- Strengthen NIEM training program for IT staff, program managers and executives
- Strengthen the tools in support the implementation of NIEM across the Department
- Develop streamlined privacy and security process for the implementation of data accessibility
- Improve Department-wide visibility for data within the Screening, Law Enforcement, Infrastructure and Intelligence functional areas

Enterprise Initiatives for the Mid-term (2-3 years):

- Develop DHS Enterprise solution for Attribute Based Access Control as part of the DHS ISE Common Framework, compliant with PM-ISE Target Architecture
- Ensure NIEM adoption across the Enterprise for all relevant information exchange activities.
- Implement streamlined privacy and security process for the implementation of data accessibility
- Improve Department-wide visibility for data within the Benefits Administration, Domain Awareness, Securing and Incident Management functional areas

Enterprise Initiatives for the Long-term (4-5 years):

- Implement DHS Enterprise solution for Attribute Based Access Control (as part of the Common Framework) that is compliant with PM-ISE Target Architecture
- Ensure data for Screening, Law Enforcement, Infrastructure, Intelligence, Benefits Administration, Domain Awareness, Securing and Incident Management functional areas are visible, understandable, accessible, trusted, and interoperable within DHS ISE and compliant with the PM-ISE Target Architecture

2.1.4: Achieve interoperability with DHS Stakeholders – Successfully achieving the strategic goal of strengthening information sharing relies on achieving interoperability of systems with DHS stakeholders for bidirectional information exchange.

Metrics for determining successful implementation of this priority include:

- Percentage of DHS SBU portals transitioned to SBU portal architecture
- Percentage of NIEM based DHS Enterprise SOA conformant information sharing services accessible within Screening, Law Enforcement, Infrastructure, Intelligence, Benefits Administration, Domain Awareness, Securing and Incident Management functional areas
- Percent Compliance with PM-ISE Functional Standards and DHS Portal Standards
- Percent of grants issued with data and wireless standards language
- Percentage of external users accessing DHS information via identity and access trust federation
- Percentage of DHS information shared with external partners that is accessed on a "self-serve" basis

Enterprise Initiatives for the Near-Term (within one year):

- Develop Grants language for Data and Wireless standards

Enterprise Initiatives for the Mid-term (2-3 years):

- Implement SBU Portal Consolidation.
- Complete deployment of HSDN to all recognized State Fusion Centers

Enterprise Initiatives for the Long-term (4-5 years):

- Implement HSDN Collaboration Tools
- Establish Screening, Law Enforcement, Infrastructure, Intelligence, Benefits Administration, Domain Awareness, Securing and Incident Management interoperability with federal, state and local stakeholders.

Objective 2.2: Enhanced DHS Person Screening and Credentialing Capabilities

Within the eleven functional areas, the Department is moving forward with specific initiatives to improve operations and effectiveness, and has issued specific policy and guidance to implement these initiatives.

Specifically, the Department has issued guidance for implementation of two key initiatives, the Credentialing Framework Initiative (CFI) and the PCV.

As part of the CFI, DHS Screening Coordination Office (SCO), in coordination with the DHS OCIO, developed specific enterprise standards and target capabilities to be implemented in order to rationalize and enhance DHS person screening and credentialing capabilities. The CFI relates the target capabilities to specific DHS programs. The DHS IT community will develop specific implementation plans to support achievement of these targets for the Screening functional area.

DHS, at the direction of the Deputy Secretary, is developing a foundation that will support a "person-centric view" of information within the Department. This initiative will create the ability to associate relevant information about a person across DHS Components and stakeholders. The appropriate DHS decision-maker will then have the information necessary and pertinent to make an informed decision, consistent with privacy and civil liberty requirements. The PCV initiative will also assist DHS in harmonizing Component investments and programs, and will streamline privacy, regulatory, and paperwork reduction access processes.

Metrics for determining successful implementation of this priority include:

- Number of targets established
- Percentage of investments developing transition plans to move towards the targets
- Percentage of investments/systems that have migrated to the established targets

Enterprise Initiatives for the Near-Term (within one year):

- Develop transition strategies for achieving CFI targets

Enterprise Initiatives for the Mid-term (2-3 years):

- Execute PCV pilots

Enterprise Initiatives for the Long-term (3-4 years):

- Execute full implementation of PCV and CFI across the Department

GOAL 3: *Improve transparency and accountability through effective governance of cross-departmental IT portfolios.*

As the complexity of the IT environment continues to grow every year, it becomes increasingly difficult for managers to know whether or not they are making well-informed IT investment decisions. It is the OCIO's responsibility to ensure a sound governance process that facilitates the best possible investment decisions and management of IT spending.

DHS is leading efforts to improve efficacy and performance across all major IT investments and increase integration from the planning phase through the O&M phase. Through effective governance, DHS aims to accomplish the following:

- Increase transparency and strengthen accountability for quantifiable program results and benefits of all major IT investments
- Extend Department-wide portfolio management in the IT governance process
- Establish segment architectures for priority mission and operational areas

The CIO will harness DHS' collective IT capabilities and assets to optimize utilization across operational, technical, and mission priorities.

The CIO is responsible for ensuring IT investments and acquisitions align to and support the needs of the DHS missions as defined by the Strategic Requirements Planning Process and the Department's Enterprise Business Architecture. The DHS OCIO is leading efforts to implement an IT governance process that facilitates sound investment decision-making and management of IT spending across the Department. Accomplishing this goal will require a structured, portfolio-based approach to managing IT, in alignment with mission priorities as defined by the DHS Office of Strategic Plans in coordination with the DHS Components. The CIO will broker the delivery of IT capabilities across by the Components by identifying, cataloging, and promoting asset reuse throughout the Department.

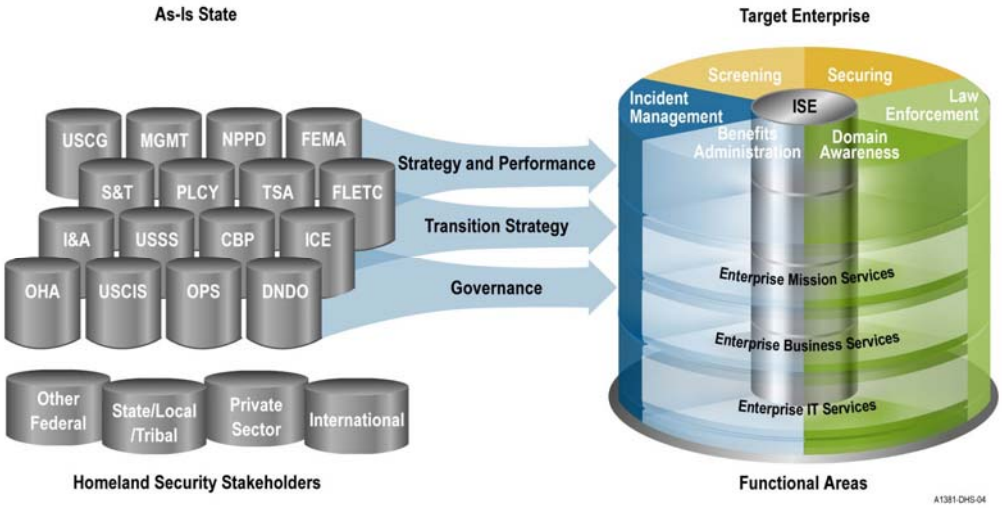

Figure 3: As-is and Target Enterprise for DHS

Objective 3.1: Integrated Departmental Governance

At DHS, IT governance consists of organizational structures and processes established to ensure that IT is aligned with and sustain the Department's mission, goals, and objectives. IT governance integrates existing best practices within the OCIO and aligns them with other Department-wide policies, processes, and tools. This ensures the Department is able to make the best possible investment decisions by taking full advantage of information, maximizing benefits, and capitalizing on opportunities for the Department.

OCIO is leading efforts to integrate all IT governance processes across the Department in order to enhance the IT investment decision-making process and to help improve program performance while reducing the burden of data calls and reporting. The DHS OCIO, in partnership with the other DHS CXOs, (including OCFO, OCPO, OCAO, etc.) is currently in the process of defining the Department's IT Governance framework.

The IT priorities in support of establishing enhanced governance across the Department include:

3.1.1: Institutionalize effective IT Governance and improved transparency of all IT investments – As DHS matures organizationally, it becomes increasingly important to institutionalize effective IT governance and improve transparency of IT investments as these will ultimately lead to improved mission and business performance.

Metrics for determining successful implementation of this priority include:

- Percentage of IT programs performing within 10% of Cost, Schedule and Performance objectives
- Percentage of Components investments following the Systems Engineering Life Cycle (SELC).
- Percentage of IT projects reporting thought nPRS
- Percent of IT investments aligned to EA targets within functional areas
- Percentage of DHS IT investments on the Management Watch List and High Risk List
- Percentage of IT investments reviewed and approved through the Strategic Requirements Planning Process, Planning, Programming, Budgeting and Execution and Acquisition Review Process and the Enterprise Architecture Board processes

Enterprise Initiatives for the Near-Term (within one year):

- Align Component processes (e.g., SLC, SDLC, SLM, ITLM) to the DHS SELC published as part of Directive 102-01
- Develop an IT Governance roadmap for IT Portfolios, integrated into DHS governance processes with mission sponsorship for each portfolio.
- Incorporate section 508 compliance reviews into Components' governance processes
- Develop the technical architecture to support the enterprise financial capability (TASC)
- Align the DHS EAB and EACOE processes to Directive 102-01
- Fully deploy nPRS and pilot federated decision support capability (SMART)

Enterprise Initiatives for the Mid-term (2-3 years):

- Develop and then implement a DHS IT Governance Implementation Framework (using CMMI, ITIL, CobiT for best practice)
- Establish federated decision support capability
- Implement initial operating capability for TASC (financial systems consolidation)
- Establish an enterprise-wide CCB

Enterprise Initiatives for the Long-term (4-5 years):

- Implement full operating capability for TASC (including support for activity based costing into program execution)
- Implement full operating capability for SMART

3.1.2: Improve Collaboration among the CXOs – Improving program performance across the enterprise is dependent on collaboration among the CXOs, each of whom has responsibilities for areas of the PPBE process. With authority over the Department's IT spending, the OCIO will collaborate with the CXOs to ensure alignment of IT management and IT governance practices with those of the Department.

Metrics for determining successful implementation of this priority include:

- Percentage of acquisition reviews completed on time
- Participation rates for Joint Governance Initiatives/Boards at HQ and Components

Enterprise Initiatives for the Near-Term (within one year):

- Aligning goals among the CXO community (HQ and Component)
- Joint efforts to focus on the end-customer
- Integration of governance processes for improved decision support

Objective 3.2: Enhanced Departmental IT Strategic Sourcing and Vendor Management Capabilities

Alignment with the management efforts across all CXOs is imperative for optimizing management capabilities across the Department. To strengthen the practice of contracts management across the enterprise, the OCIO will leverage the Department's Strategic Sourcing Capability and will implement performance-based contract management and vendor management best practices.

Metrics for determining successful implementation of this priority include:

- Percentage of enterprise strategic sourcing contracts established for enterprise IT services
- Percentage of IT programs using standardized Departmental chart of accounts

Enterprise Initiatives for the Near-Term (within one year):

- Utilize enterprise contract vehicles and enterprise license agreements to support Data Center consolidation and O&M
- Establish an enterprise cost model for stewardship activities and framework for funding service-level management

Enterprise Initiatives for the Mid-term (2-3 years):

- Pilot operating, funding, acquisition model for enterprise IT services

Objective 3.3: Enhanced Communications

The OCIO is working to improve its Strategic Communications efforts in order to better communicate to external stakeholders and the public the positive impacts the Department is making. This effort is also important in ensuring that programs are more aware of what is required of them for reporting purposes. It will also help ensure programs have adequate time to plan for review processes and responses to for-the-record questions, IG/OMB/GAO reports, and IT community reports. Additionally, the Department is striving to improve customer satisfaction and increase efficiency of existing processes through enhanced communications.

The OCIO will improve communications channels and implement bi-directional internal and external communications by using Web 2.0 collaboration technology.

Metrics for determining successful implementation of this priority include:

- Having strategic Communications included as a core competency for CIO Offices
- Scores on the DHS PMA and eGOV Scorecard

Enterprise Initiatives for the Near-Term (within one year):

- Develop a proactive approach for communication with active stakeholder management
- Publish a strategic communications plan
- Develop a Web 2.0 strategy

Enterprise Initiatives for the Mid-term (2-3 years):

- Implement the communications strategy across the enterprise
- Conduct customer satisfaction surveys
- Pilot the Web 2.0 capability

Enterprise Initiatives for the Long-term (4-5 years):

- Fully implement its Web 2.0 capability

GOAL 4*: Develop and implement a comprehensive approach to IT employee recruitment, development, retention, and recognition to ensure excellence in IT delivery across the Department.*

To attract and retain high-performing IT staff, it is incumbent upon the OCIO to develop a comprehensive strategy around recruiting and retaining the Department's IT workforce. The OCIO is in the process of developing policies and procedures for IT staff recruitment and development that are aligned with Office of the Chief Human Capital Officer's (CHCO) policies to increase staff retention, reduce turnover, and promote excellence in IT delivery.

IT enables program success and a key to delivering world-class IT capabilities is through attraction, retention, and growth of skilled government technology staff that can manage and oversee the partnership of DHS with top commercial and government providers of DHS technology services. It is also critical for DHS to continue to recruit and retain top-level staff to fill key IT positions including enterprise architects, program and project managers, IT security managers, and contracting officers with a deep understanding of IT contracting requirements. Most important, DHS must retain top performers interested in upward movement into key managerial and executive positions and, accordingly, DHS must make available for its IT professionals an attractive career path.

The trend in Government has shifted towards outsourcing most technology implementation and operational work to commercial and other Government service providers. As such, DHS IT staff must continue to provide key leadership and direction to the Department's IT program.

Objective 4.1: Comprehensive and Effective IT Human Capital Management

A comprehensive Human Capital Management strategy will promote continuous growth and development of IT staff skill sets, ensuring the Department provides leading IT capabilities. The OCIO has increased its focus on IT workforce training as it is critical to DHS' success and impacts most of the Department's other goals and objectives.

The IT priorities in support of attaining this objective include:

4.1.1: Develop and Implement an Integrated DHS IT Human Capital Plan - The OCIO will work with the Component CIOs and the DHS CHCO to develop a workforce plan that will detail the strategy for enhancing the DHS IT workforce.

Metrics for determining successful implementation of this priority include:

- Implementation of an approved plan across all Directorates within OCIO and Components

Enterprise Initiatives for the Near-Term (within one year):

- Develop an IT Human Capital Plan
- Establish an IT Workforce JPMO
- Implement E-Recruitment across the Enterprise

Enterprise Initiatives for the Mid-term (2-3 years):

- Implement the IT Human Capital plan.
    - This plan will include the following sections: 1) DHS IT Career Path, 2) Rotational Assignments, 3) Improved hiring/ clearance process, 4) IT Training Strategy, and 5) Improved recruitment and retention of IT staff.

Enterprise Initiatives for the Long-term (4-5 years):

- Deploy the E-Recruitment Initiative across the enterprise

4.1.2: Improve Staff Retention and Career Planning: As the IT community matures, beyond establishing a Human Capital Plan for IT staff, the OCIO will need to demonstrate an improvement in staff retention. It will also need to display the availability of career planning (and succession planning) to map a clear and desirable career path for DHS IT professionals. These efforts will include a mentoring program. Leadership within the IT Community is currently working to ensure that incentives are provided for staff to advance and stay competitive in the marketplace. Additionally, across DHS, Leadership has been focusing on making the DHS career paths competitive with other agencies (i.e. FBI), as well as the commercial sector.

Metrics for determining successful implementation of this priority include:

- Percentage improvement in retention rates
- Percentage decrease in "recruiting-to-on boarding" timeframe
- Percentage of Individual Development Plans (IDP) developed for IT personnel used to manage career paths
- Number of internal promotions versus external hires
- Number of Mentoring candidates

Enterprise Initiatives for the Near-Term (within one year):

- Develop an IT Acquisition Management curriculum for level 1 and 2 IT program managers

Enterprise Initiatives for the Mid-term (2-3 years):

- Roll-out the programs identified in the Human Capital plan noted above
- Carry out the activities identified by the JPMO to enhance the DHS IT workforce

Enterprise Initiatives for the Long-term (4-5 years):

- Continue to enhance its processes related to recruitment and retention of an excellent IT workforce
- Continue to deliver leading IT capabilities, such as E-Recruitment

5.0 Conclusion

This IT Strategic Plan is intended to help improve strategic planning for IT across the Department and to integrate the Department's IT Community through unification of cross-Component IT priorities. This plan serves as the foundation for the IT portion of the DHS IPG for FY 2011-2015 and will aid Components in appropriately planning their IT budgets.

Implementation of the priorities and initiatives in this plan rely on DHS' continued commitment to operational excellence, stronger collaboration across CXOs, and integration of governance processes. The continued maturity of processes, such as the recently established Directive 102-01, across DHS will also help improve program performance. With various organizations across the Department at different levels of organizational maturity, there is ample opportunity to leverage best practices and implement the best possible solutions.

This plan's call to action is for IT to help DHS achieve higher levels of mission performance within budgetary constraints and to take a more coordinated approach to sharing business solutions and information. The goal is to make the DHS IT organization more effective and to better serve business users and citizens, by achieving better use of IT dollars and enterprise solutions.

6.0 Appendices

Appendix A: Authorities and Guidance

Federal Guidance	*Departmental Guidance*
• National Strategy for Homeland Security	• DHS Strategic Plan
• Clinger-Cohen Act	• DHS IT Strategic Plan
• Electronic Government Act	• DHS Directive 102-01 Acquisition Management
• Executive Order 13011 Federal Information Technology	• DHS Management Directive 0007.1 Information Technology Integration and Management
• Federal Information Security Management Act	• DHS Management Directive 4300 A, DHS Sensitive Systems Policy and Handbook
• Federal Records Act	• Homeland Security Enterprise Architecture (HLS EA)
• Freedom of Information Act • Government Performance and Reports Act	• DHS Directive 103-01 Acquisition Line of Business
• OMB Circular A-11, Part 7 – Capital Planning Budget Reporting, Exhibits 52, 53, and 300	
• OMB Circular A-130, Management of Federal Information Resources, Section 8b	
• President's Management Agenda	
• Privacy Act	
• Public Printing and Documents, Federal Information Policy (U.S. Code Title 44)	
• Public Law 105-220, Section 508 of the Rehabilitation Act of 1973, as amended in the Workforce Investment Act of 1998	
• PL 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, Title V—Improving Intelligence and Information Sharing Within the Federal Government and with State, Local, and Tribal Governments	

Appendix B: List of Acronyms

ACRONYM	DESCRIPTION
ABAC	Attribute Based Access Control
AWN	Alerts, Warnings, and Notifications
BIA	Business Impact Analysis
CFI	Credentialing Framework Initiative
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
DHS-ISE	DHS Information Sharing Environment
DR	Disaster Recovery
e-Gov	E-Government
EA	Enterprise Architecture
EDS	Electronic Data Systems
ERB	EA Review Board
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GPRA	Government Performance and Results Act
HSDN	Homeland Secure Data Network
IDAM	Identity and Access Management
IDP	Individual Development Plan
IG	Inspector General
IPG	Integrated Planning Guidance
IPv6	Internet Protocol version 6
IT	Information Technology
LOB	line of business
MD	Management Directive
MOU	Memorandums of Understanding
MPLS	Multiprotocol Label Switching
NSS JPMO	National Security Systems Joint Program Management Office
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence

OMB	Office of Management and Budget
PART	Program Assessment Rating Tool
PCV	Person Centric View
PEP	Policy Enforcement Point
PM-ISE	Program Manager Information Sharing Environment
PMA	President's Management Agenda
PMO	Program Management Office
POP	points of presence
PPBE	Planning, Programming, Budgeting, and Execution
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCO	Screening Coordination Office
SELC	Systems Engineering Life Cycle
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SSO	Single Sign-On
TAF	Trusted Agent FISMA
TIC	Trusted Internet Connection
TIG	Tactical Interface Gateway
TS	Top Secret
TWL	Terrorist Watch List